

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 031 909 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
30.08.2000 Bulletin 2000/35

(51) Int. Cl.⁷: G06F 1/00

(21) Application number: 00300727.5

(22) Date of filing: 31.01.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE

Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 23.02.1999 US 256432

(71) Applicant:
Sightsound.Com Incorporated
Mt. Lebanon, PA 15228 (US)

(72) Inventor: Hair, Arthur R.
Upper St. Clair, PA 15241 (US)

(74) Representative:
O'Connell, David Christopher
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(54) A system and method for manipulating a computer file and/or program

(57) A system for manipulating a computer file and/or program. The system includes a serving device having access to a computer file and/or program which is unencrypted and which can encrypt the unencrypted computer file and/or program to become an encrypted computer file and/or program and transfer it. The system includes a connector connected to the serving device on which the encrypted computer file and/or program travels and to which the serving device transfers the encrypted computer file and/or program. The system includes a client device which receives the encrypted computer file and/or program and decrypts the encrypted computer file and/or program back to the unencrypted computer file and/or program. The client device does not allow intervention to the encrypted computer file and/or program during a time when the encrypted computer and/or file program is received. The serving device is separate, apart and distinct from the client device. A method for manipulating a computer file and/or program. The method includes the steps of suspending intervention by a user at a client device of the client device. Then there is the step of encrypting an unencrypted computer file and/or program at the server device to form an encrypted computer file and/or program. Next there is the step of transferring the encrypted computer file and/or program to the client device along a connector connected to the client device and the server device. Then there is the step of reestablishing the intervention of the client device by the user.

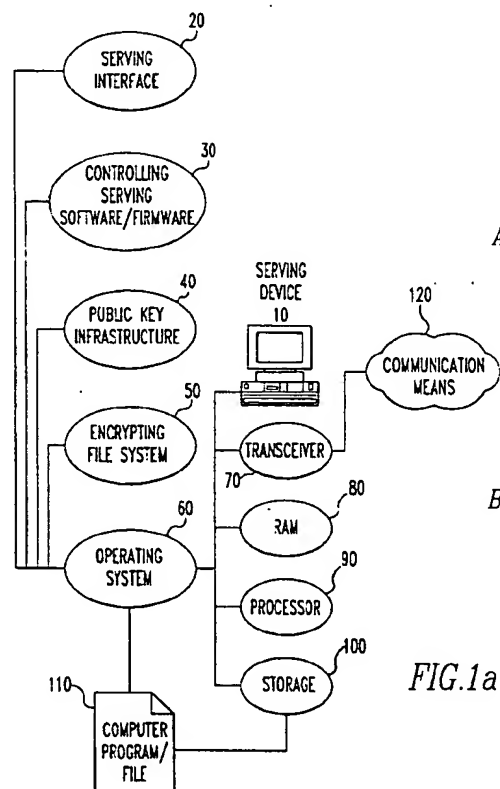


FIG.1a

EP 1 031 909 A2

Description

FIELD OF THE INVENTION

[0001] The present invention is related to a method and system to automatically invoke functionality of an operating system during the encrypted transmission and encrypted storage of computer files and/or computer programs from one computing device to another computing device.

BACKGROUND OF THE INVENTION

[0002] The secure transmission of computer files via communication means has increased in importance with the proliferation of the Internet for electronic distribution and electronic commerce. The fundamental shift from physical delivery of computer files and/or computer programs to digital based electronic transmission has commenced with the Internet emerging as a ubiquitous low cost network. As in previous technological advancements such as the transition from newspaper to radio and then to television, media companies of the time were forced to react to the emergence of these new mediums. However, unlike previous technological transitions, the Internet as a medium supports all of the functionality of the traditional print, radio and television industries while simultaneously supporting electronic commerce as well. Currently, many businesses utilize the Internet to sell or give away their computer files and/or computer programs via the Internet and in most cases, the computer files are not encrypted for protection against piracy or illegal use. Additionally, the current approach relating to the secure transmission and storage of computer files fails to leverage encryption functionality of a computing device's operating system. The current approach calls for a computing device acting as a server (the "Serving Device") to communicate with another computing device acting as a client (the "Client Device") to transfer encrypted files for decryption at the application level (such as, but not limited to, Win32 Application) of the Client Device. The Client Device utilizes a computer program running at the application level for decryption, which is assigned a unique decryption "key." During the transmission process, the Serving Device encrypts the computer file for storage using the decryption "key" of the Client Device. The encrypted computer file is then transmitted via the Internet and saved into storage within, or connected to, the Client Device. After decryption of the computer file, the decrypting computer program transmits a decrypted signal to the operating system for display or, in the case of an audio file, playback through the sound card. The decrypted signal can be vulnerable when transmitted from the decrypting application to the operating system, and the signal can be intercepted, possibly resulting in the illegal duplication of the computer file.

[0003] Addressing certain aspects of computer file

and computer program encryption, the Microsoft Corporation published in 1998, a white paper titled "Microsoft Windows NT version 5.0, Public Key Infrastructure", incorporated by reference herein, (hereinafter the "Windows 2000 PKI White Paper"), detailing encryption functionality of a comprehensive public key infrastructure (PKI) in the Windows 2000 family of operating systems (formerly referred to as Windows NT 5.0). The Windows 2000 PKI White Paper stated on the cover page thereof, "Microsoft. Windows NT. version 5.0 introduces a comprehensive public key infrastructure (PKI) to the Windows. platform. This utilizes and extends the Windows-based public key (PK) cryptographic services introduced over the past few years, providing an integrated set of services and administrative tools for creating, deploying, and managing PK-based applications. This allows application developers to take advantage of the shared-secret security mechanisms or PK-based security mechanism in Windows NT as appropriate. At the same time, enterprises gain the advantage of being able to manage the environment and applications based on consistent tools and policy mechanisms."

[0004] Furthermore, and with special emphasis on the encryption functionality of the Public Key Infrastructure of the Windows 2000 family of operating systems, the Windows PKI White Paper stated, "The Web has rapidly become a key element in creating and deploying solutions for the effective exchange of information on a worldwide basis. In particular, growth in its use for business purposes has been dramatic. For many uses, security is a key consideration. Notably: Server authentication - To enable clients to verify the server they are communicating with. Client authentication - To allow servers to verify the client's identity and use this as a basis for access control decisions. Confidentiality - Encryption of data between clients and servers to prevent its exposure over public Internet links.

[0005] The Secure Sockets Layer (SSL) and the emerging IETF standard Transport Layer Security (TLS) protocols play an important role in addressing these needs. SSL and TLS are flexible security protocols that can be layered on top of other transport protocols. They rely on PK-based authentication technology and use PK-based key negotiation to generate a unique encryption key for each client and/or server session. They are most commonly associated with Web-based applications and the HTTP protocol (referred to as HTTPS).

[0006] SSL and TLS are supported on the Windows platform by the secure channel (schannel) SSPI provider. Microsoft Internet Explorer and Internet Information Services both use schannel for this functionality. Because schannel is integrated with Microsoft's SSPI architecture, it is available for use with multiple protocols to support authenticated and/or encrypted communications.

[0007] Taking full advantage of the SSL and TLS protocols requires both clients and servers to have identification certificates issued by mutually trusted CAs,

this secret key and associate it with the file. In addition, a copy of the secret key, encrypted with each recovery agent's EFS public key, is associated with the file. No plaintext copy of the secret key is stored in the system.

[0017] When retrieving the file, EFS transparently unwraps the copy of the secret key encrypted with the user's public key using the user's private key. This is then used to decrypt the file in real time during file read and write operations. Similarly, a recovery agent may decrypt the file by using the private key to access the secret key."

[0018] Providing additional detail on the level of security of Microsoft's Encrypting File System, the Windows 2000 Workstation White Paper states on page 28 thereof, "An Encrypted File System (EFS) encrypts files on a hard disk. Each file is encrypted using a randomly generated key, which is independent of the users' public and/or private key pair. EFS resides in the Windows NT kernel and uses the non-paged pool to store file encryption keys, ensuring that they never reach the paging file. EFS is supported on a file or directory basis. Encryption and decryption is transparent to the user."

[0019] The instability of computing functions (such as, but not limited to, functions resulting in computing system crashes) is generally regarded as greater at the application level than at the operating system level. The closer the computing functions are to the core of the operating system, the more stable they are generally. If an application level decryption program becomes damaged or corrupted and reinstallation of another decryption program is required, a new "decryption key" is generated and the previously encrypted computer files, being encrypted to the old "decryption key," can not be decrypted by the newly installed decryption program. Avoiding the encryption and/or decryption weaknesses inherent in application level programs, Microsoft has taken steps to protect lost "encryption and/or decryption keys" in the Windows 2000 PKI. Microsoft stated in the Windows 2000 PKI White Paper on page 14 thereof, "Public key pairs and certificates tend to have high value. If they are lost due to system failure, their replacement may be time consuming and result in monetary loss. To address these issues, the Windows NT 5.0 PKI supports the ability to back up and restore both certificates and associated key pairs through the certificate-management administrative tools."

SUMMARY OF THE INVENTION

[0020] The present invention offers a new and improved method and system to automatically invoke certain functionality of a public key infrastructure and encrypting file system of operating systems to encrypt computer files or computer programs for electronic transmission between computing devices and encrypt those computer files or computer programs for subsequent storage, and restrict usage permissions and/or rights. The present invention instructs the operating

systems of the computing devices to temporarily suspend user intervention until completion of the encrypted transmission and encrypted storage process to prevent unauthorized use of replication of the computer files or computer programs. The present invention instructs the public key infrastructure of a serving device to encrypt for transmission a computer file or computer program (and any accompanying permissions and/or rights established by the serving device) stored within, or connected to, the serving device then transmit said computer file or computer program to the client device. Upon receipt by the client device of said computer file or computer program (and any accompanying permissions and/or rights established by the serving device), the present invention automatically instructs the public key infrastructure of the client device to decrypt from transmission said computer file or computer program (and any accompanying permissions and/or rights established by the serving device) transmitted by the serving device. The present invention then instructs the encrypting file system of the client device to encrypt for storage, based on any permissions and/or rights as established by the serving device and which accompanied the computer file or computer program, and store the computer file or computer program. The present invention separates the storage encryption process from the transmission encryption process to enable encrypted transmission between computing devices running different operating systems, using industry standard communication protocols, then having the different operating systems execute their unique or proprietary storage encryption process. Furthermore, the most widely used operating systems support the encrypted transmission standards of the Internet, however, standards do not exist for operating system based encrypted storage. A unique benefit of the present invention is that it utilizes multiple encryption and/or decryption processes to provide an end-to-end solution for the encrypted transfer and storage of computer files and/or programs between computers running different operating systems. Instead of permanently encrypting a computer file and/or program for use on one specific decrypting device or computer, the present invention assigns permissions and/or rights to the computer file and/or program then tasks the encryption functionality of operating system possessing the computer file and/or program to enforce the permissions and/or rights. In this way, flexible permissions and/or rights can be assigned to the computer file and/or program which follow it from computer to computer, from operating system to operating system, while being encrypted and decrypted, as necessary, along the way.

[0021] The present invention also offers a new and improved method and system to activate certain functionality of a public key infrastructure and encrypting file system of the client device to execute any permissions and/or rights which accompanied a given computer file or computer program. Permissions and/or rights (such

gram which may also be used in carrying out the teachings of this invention for the purposes of automatically invoking functionality of the Operating System 62 of the Client Device 12 to: receive and decrypt a Computer File and/or Program 110, and its associated permissions and/or rights, from transmission from a Client Device 11 through use of a Transceiver 72 connected to a Communication Means 120 and store an electronic copy thereof in RAM 82; encrypt and save said Computer File and/or Program 110 from RAM 82 to Storage 102 using said associated permissions and/or rights, and then erase any electronic copies of said Computer File and/or Program 110 from RAM 82; and

Fig. 3 is a computer programming flowchart which may be used in carrying out the teachings of this invention for the purpose of automatically invoking functionality of the Operating System 60 of the Serving Device 10 to: encrypt and transmit a Computer File and/or Program 110, and its associated permissions and/or rights, to a Client Device 11 through use of a Transceiver 70 connected to a Communication Means 120. Fig. 3 is a computer programming flowchart which may also be used in carrying out the teachings of this invention for the purpose of automatically invoking functionality of the Operating System 61 of the Client Device 11 to: receive and decrypt a Computer File and/or Program 110, and its associated permissions and/or rights, from transmission from a Serving Device 10 through use of a Transceiver 71 connected to a Communication Means 120 and store an electronic copy thereof in RAM 81; encrypt and save said Computer File and/or Program 110 from RAM 81 to Storage 101 using said associated permissions and/or rights, and then erase any electronic copies of said Computer File and/or Program 110 from RAM 81; and

Fig. 4 is a computer programming flowchart which may be used in carrying out the teachings of this invention for the purposes of automatically invoking functionality of the Operating System 61 of the Client Device 11 to: decrypt a Computer File and/or Program 110 from Storage 101 and store an electronic copy thereof, and store the associated permissions and/or rights, in RAM 81; and encrypt and transmit a Computer File and/or Program 110, and its associated permissions and/or rights, to a Next Client Device 11 through use of a Transceiver 71 connected to a Communication Means 120; and then erase any electronic copies of said Computer File and/or Program 110 from RAM 81; and, in the case of a move of said Computer File and/or Program 110 from Storage 101 to Storage 102, then erase any electronic copies of said Computer File and/or Program 110 from Storage 101. Fig. 4 is a computer programming flowchart which may also be used in carrying out the teachings of this inven-

tion for the purposes of automatically invoking functionality of the Operating System 62 of the Client Device 12 to: receive and decrypt a Computer File and/or Program 110, and its associated permissions and/or rights, from transmission from a Client Device 11 through use of a Transceiver 72 connected to a Communication Means 120 and store an electronic copy thereof in RAM 82; encrypt and save said Computer File and/or Program 110 from RAM 82 to Storage 102 using said associated permissions and/or rights, and then erase any electronic copies of said Computer File and/or Program 110 from RAM 82.

DETAILED DESCRIPTION

[0025] Referring now to the drawings wherein like reference numerals refer to similar or identical parts throughout the several views, and more specifically to Figures 1 and 2 thereof, there is shown a system for manipulating a computer file and/or program. The system comprises a serving device 10 having access to a computer file and/or program which is unencrypted and which can encrypt the unencrypted computer file and/or program to become an encrypted computer file and/or program and transfer it. The system comprises a connector connected to the serving device 10 on which the encrypted computer file and/or program travels and to which the serving device 10 transfers the encrypted computer file and/or program. The connector can be communication means 120. The system comprises a client device 11 which receives the encrypted computer file and/or program and decrypts the encrypted computer file and/or program back to the unencrypted computer file and/or program. The client device 11 does not allow intervention to the encrypted computer file and/or program during a time when the encrypted computer and/or file program is received. The serving device 10 is separate, apart and distinct from the client device 11.

[0026] Preferably, the server device assigns permissions and/or rights to the unencrypted computer file and/or program which identifies what the client device 11 can do with the unencrypted or encrypted computer file and/or program after the client device 11 has received the encrypted computer file and/or program or after the client device 11 has decrypted the encrypted computer file and/or program back to the unencrypted computer file and/or program. The server device preferably encrypts the permissions and/or rights and transfers them to the client device 11 through the connector. The client device 11 decrypts the unencrypted permissions and/or rights.

[0027] Preferably, the serving device 10 includes controlling server software and/or firmware 30 which causes the encryption of the unencrypted computer file and/or program and the permissions and/or rights and instructs the client device 11 to temporarily suspend user intervention when the client device 11 receives the

means or mechanism for invoking functionality of an Operating System 61 of a Client Device 11 to: instruct the Operating System 61 to temporarily suspend user intervention of the Client Device 11 during the execution of the functionality of the apparatus 30 and 31; conduct encrypted communications through use of a Transceiver 70 connected to a Communication Means 120; receive and decrypt a Computer File and/or Program 110, and its associated permissions and/or rights, from transmission from a Serving Device 10 through use of a Transceiver 71 connected to a Communication Means 120 and store an electronic copy thereof in RAM 81; encrypt and save said Computer File and/or Program 110 from RAM 81 to Storage 101 using said associated permissions and/or rights, and then erase any electronic copies of said Computer File and/or Program 110 from RAM 81; instruct the Operating System 61 to restore user intervention of the Client Device 11 upon completion of the execution of the functionality of the apparatus 30 and 31.

[0035] Referring now to the drawings wherein like reference numerals refer to similar or identical parts throughout the several views, and more specifically to Fig. 2 and Fig. 4 thereof, there is shown apparatuses 31 and 32 for invoking functionality of the Operating Systems 61 and 62 of computing devices Client Device 11 and Next Client Device 12, respectively. The apparatuses 31 and 32 are connected to the Operating Systems 61 and 62 of computing devices Client Device 11 and Next Client Device 12, respectively. The apparatus 31 comprises a means or mechanism for invoking functionality of an Operating System 61 of a Client Device 11 to: instruct the Operating System 61 to temporarily suspend user intervention of the Client Device 11 during the execution of the functionality of the apparatus 31 and 32; instruct the apparatus 32 to instruct the Operating System 62 to temporarily suspend user intervention of the Next Client Device 12 during the execution of the functionality of the apparatus 31 and 32; conduct encrypted communications through use of a Transceiver 71 connected to a Communication Means 120; decrypt a Computer File and/or Program 110 from Storage 101 and store an electronic copy thereof, and store the associated permissions and/or rights, in RAM 81; encrypt and transmit a Computer File and/or Program 110, and its associated permissions and/or rights, to a Next Client Device 12 through use of a Transceiver 71 connected to a Communication Means 120; and then erase any electronic copies of said Computer File and/or Program 110 from RAM 81; and, in the case of a move of said Computer File and/or Program 110 from to Storage 101 to Storage 102, then erase any electronic copies of said Computer File and/or Program 110 from Storage 101; instruct the Operating System 61 to restore user intervention of the Client Device 11 upon completion of the execution of the functionality of the apparatus 31.

[0036] The apparatus 32 comprises a means or

mechanism for invoking functionality of an Operating System 62 of a Next Client Device 12 to: instruct the Operating System 62 to temporarily suspend user intervention of the Next Client Device 12 during the execution of the functionality of the apparatus 31 and 32; conduct encrypted communications through use of a Transceiver 71 connected to a Communication Means 120; receive and decrypt a Computer File and/or Program 110, and its associated permissions and/or rights, from transmission from a Client Device 11 through use of a Transceiver 72 connected to a Communication Means 120 and store an electronic copy thereof in RAM 82; encrypt and save said Computer File and/or Program 110 from RAM 82 to Storage 102 using said associated permissions and/or rights, and then erase any electronic copies of said Computer File and/or Program 110 from RAM 82; instruct the Operating System 62 to restore user intervention of the Next Client Device 12 upon completion of the execution of the functionality of the apparatus 32.

[0037] Referring now to Fig. 1 and Fig. 3, one preferred embodiment of the invention is comprised of the following:

25	10	Serving Device
	11	Client Device
	20	Serving Interface
	21	Client Interface
	3	Controlling Serving Software and/or Firmware (also "Serving CSS and/or F")
30	31	Controlling Client Software and/or Firmware (also "Client CCS and/or F")
	40	Public Key Infrastructure
	41	Public Key Infrastructure
35	50	Encrypting File System
	51	Encrypting File System
	60	Operating System
	61	Operating System
	70	Transceiver
40	71	Transceiver
	80	Random Access Memory (also "RAM")
	81	Random Access Memory (also "RAM")
	90	Processor
	91	Processor
45	100	Storage
	101	Storage
	110	Computer File and/or Program (also "File and/or Program")
	120	Communication Means

[0038] In Fig. 1 and Fig. 3, the following components are already commercially available: the Serving Device 10, the Client Device 11, the Serving Interface 20, the Client Interface 21, the Public Key Infrastructure 40, the Public Key Infrastructure 41, the Encrypting File System 50, the Encrypting File System 51, the Operating System 60, the Operating System 61, the Transceiver 70, the Transceiver 71, the Random Access

establish third party usage permissions and/or rights to be associated with a Computer File and/or Program 110 thereby limiting the usage of the Computer File and/or Program 110 by the Client Device 11 or the Next Client Device 12. The Controlling Serving Software and/or Firmware 30 is also a means or mechanism to automatically instruct a Public Key Infrastructure 40 of a Serving Device 10 to encrypt and transmit usage permissions and/or rights associated with a Computer File and/or Program 110 and to encrypt and transmit a Computer File and/or Program 110 to a Client Device 11 via Communication Means 120. The Controlling Serving Software and/or Firmware 30 may be embodied in computer coding software (such as, but not limited to, a program authored in the computer language c++) to execute the described functions).

[0048] The Controlling Client Software and/or Firmware 31 is a means or mechanism to automatically instruct the Operating System 61, or a communication program thereof, to communicate with a Serving Device 10 or a Next Client Device 12 via Communication Means 120. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to receive instructions from a Controlling Serving Software and/or Firmware 30 via Communication Means 120. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to instruct the Operating System 61 to temporarily suspend user intervention of the Client Device 11 during the execution of the functionality of the Controlling Serving Software and/or Firmware 30 and the Controlling Client Software and/or Firmware 31. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to automatically instruct a Public Key Infrastructure 41 of a Client Device 11 to receive and decrypt from transmission usage permissions and/or rights associated with a Computer File and/or Program 110 and to receive and decrypt from transmission a Computer File and/or Program 110 transmitted from a Serving Device 10 via Communication Means 120 and place an electronic copy thereof in RAM 81. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to automatically instruct the Encrypting File System 51 of a Client Device 11 to recall a Computer File and/or Program 110 from RAM 81 and encrypt and save an electronic copy thereof to Storage 101, using said permissions and/or rights associated with said Computer File and/or Program 110 and transmitted by the Serving Device 10. The Controlling Client Software and/or Firmware 31 is a means or mechanism to instruct the Operating System 61 to restore user intervention of the Client Device 11 upon completion of the execution of the functionality of the Controlling Serving Software and/or Firmware 30 and Controlling Client Software and/or Firmware 31. The Controlling Client Software and/or Firmware 31 is a means or mechanism to instruct the Operating System 61 to temporarily suspend user intervention of the Client Device 11 during execution of the functionality of the

Controlling Client Software and/or Firmware 31 and Controlling Client Software and/or Firmware 32. The Controlling Client Software and/or Firmware 31 is a means or mechanism to instruct the Controlling Client Software and/or Firmware 32 to instruct the Operating System 62 to temporarily suspend user intervention of the Next Client Device 12 during execution of the functionality of the Controlling Client Software and/or Firmware 31 and Controlling Client Software and/or Firmware 32. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to receive instructions from a Controlling Client Software and/or Firmware 32 of a Next Client Device 12 via Communication Means 120. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to automatically instruct the Encrypting File System 51 of a Client Device 11 to decrypt a Computer File and/or Program 110 from Storage 101 and place an electronic copy thereof in RAM 81. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to automatically instruct the Public Key Infrastructure 41 of a Client Device 11 to encrypt and transmit via Communication Means 120 a Computer File and/or Program 110 to a Next Client Device 12. The Controlling Client Software and/or Firmware 31 is also a means or mechanism to instruct the Operating System 61 to restore user intervention of the Client Device 11 upon completion of the execution of the functionality of the Controlling Client Software and/or Firmware 31. The Controlling Client Software and/or Firmware 31 may be embodied in computer coding software (such as, but not limited to, a program authored in the computer language c++) to execute the functions described hereinabove. The Controlling Client Software and/or Firmware 31 has many embodiments similar to those of the Controlling Client Software and/or Firmware 32.

[0049] The Controlling Client Software and/or Firmware 32 is a means or mechanism to automatically instruct the Operating System 62, or a communication program thereof, to electronically communicate with a Client Device 12 via Communication Means 120. The Controlling Client Software and/or Firmware 32 is also a means or mechanism to receive instructions from a Controlling Client Software and/or Firmware 31, of a Client Device 11, via Communication Means 120. The Controlling Client Software and/or Firmware 32 is also a means or mechanism to instruct the Operating System 62 to temporarily suspend user intervention of the Next Client Device 12 during the execution of the functionality of the Controlling Client Software and/or Firmware 31 and the Controlling Client Software and/or Firmware 32. The Controlling Client Software and/or Firmware 32 is also a means or mechanism to automatically instruct the Public Key Infrastructure 42 of a Next Client Device 12 to receive and decrypt from transmission, usage permissions and/or rights associated with a Computer File and/or Program 110 and to receive and decrypt from transmission a Computer File and/or Program 110

said randomly generated secret encryption and/or decryption key associated with said Computer File and/or Program 110 using the private decryption key of the Public Key Infrastructure 41 to then decrypt said Computer File and/or Program 110 using said randomly generated secret encryption and/or decryption key in real time during read and write operations of the Client Device 11.

[0055] The Encrypting File System 52 (such as, but not limited to, the Encrypting File System of Microsoft Windows 2000 professional, formerly known as Microsoft Windows NT Workstation version 5.0) is a means or mechanism to permit the user of a Next Client Device 12 to manually select computer files or folders to encrypt or decrypt. The Encrypting File System 52 is also a means or mechanism to encrypt a Computer File and/or Program 110 using a randomly generated and secret encryption and/or decryption key. The Encrypting File System 52 is also a means or mechanism to encrypt said randomly generated secret encryption and/or decryption key using the public encryption key of the Public Key Infrastructure 42 and save it to Storage 102 and associating said randomly generated secret encryption and/or decryption key with said Computer File and/or Program 110. The Encrypting File System 52 is also a means or mechanism to decrypt the copy of said randomly generated secret encryption and/or decryption key associated with said Computer File and/or Program 110 using the private decryption key of the Public Key Infrastructure 42 to then decrypt said Computer File and/or Program 110 using said randomly generated secret encryption and/or decryption key in real time during read and write operations of the Next Client Device 12.

[0056] The Operating System 60 (such as, but not limited to, the Microsoft Windows 2000 Server, formerly known as Microsoft Windows NT Server version 5.0) is a means or mechanism to permit computing functionality of a Serving Device 10.

[0057] The Operating System 61 (such as, but not limited to, the Microsoft Windows 2000 professional, formerly known as Microsoft Windows NT Workstation version 5.0) is a means or mechanism to permit computing functionality of a Client Device 11.

[0058] The Operating System 62 (such as, but not limited to, the Microsoft Windows 2000 professional, formerly known as Microsoft Windows NT Workstation version 5.0) is a means or mechanism to permit computing functionality of a Next Client Device 12.

[0059] The Transceiver 70 (such as, but not limited to, a modem, cable modem, network interface card, etc.) is a means or mechanism to electronically send and receive communication signals via a Communication Means 120. The Transceiver 70 is a means or mechanism used by software and/or firmware of, or connected to, the Serving Device 10 and/or the Operating System 60, to electronically communicate via a Communication Means 120. The Transceiver 70 is con-

nected to the Serving Device 10 and is connected to the Communication Means 120.

[0060] The Transceiver 71 (such as, but not limited to, a modem, cable modem, network interface card, etc.) is a means or mechanism to electronically send and receive communication signals via a Communication Means 120. The Transceiver 71 is a means or mechanism used by software and/or firmware of, or connected to, the Client Device 11 and/or the Operating System 61, to electronically communicate via a Communication Means 120. The Transceiver 71 is connected to the Client Device 11 and is connected to the Communication Means 120.

[0061] The Transceiver 72 (such as, but not limited to, a modem, cable modem, network interface card, etc.) is a means or mechanism to electronically send and receive communication signals via a Communication Means 120. The Transceiver 72 is a means or mechanism used by software and/or firmware of, or connected to, the Next Client Device 12 and/or the Operating System 62, to electronically communicate via a Communication Means 120. The Transceiver 72 is connected to the Next Client Device 12 and is connected to the Communication Means 120.

[0062] The Random Access Memory 80 (also "RAM 80") is a means or mechanism used by the Operating System 60 of a Serving Device 10 to temporarily store computer files, computer programs or other computer information for use by the Operating System 60, computer programs running on the Operating System 60 or other computer peripheral devices of said Serving Device 10.

[0063] The Random Access Memory 81 (also "RAM 81") is a means or mechanism used by the Operating System 61 of a Client Device 11 to temporarily store computer files, computer programs or other computer information for use by the Operating System 61, computer programs running on the Operating System 61 or other computer peripheral devices of said Client Device 11.

[0064] The Random Access Memory 82 (also "RAM 82") is a means or mechanism used by the Operating System 62 of a Next Client Device 12 to temporarily store computer files, computer programs or other computer information for use by the Operating System 62, computer programs running on the Operating System 62 or other computer peripheral devices of said Next Client Device 12.

[0065] The Processor 90 is a means or mechanism of a Serving Device 10 to electronically process instructions of the Operating System 60, other computer programs running on said Operating System 60 or other computer peripheral devices of said Serving Device 10. The Processor 90 is also a means or mechanism of a Serving Device 10 to electronically process instructions of other peripheral software and/or firmware devices of said Serving Device 10.

[0066] The Processor 91 is a means or mechanism

Serving Software and/or Firmware 30 to transmit the Computer File and/or Program 110 to the Client Device 11. Then the Controlling Serving Software and/or Firmware 30 instructs the Public Key Infrastructure 40 of the Operating System 60 of the Serving Device 10 to encrypt and transmit, using encrypted communication protocols (such as, but not limited to, secure sockets layer (SSL), transport layer security (TLS), virtual private network (VPN), etc.), the Computer File and/or Program 110 and its associated permissions and/or rights to the Client Device 11. Then the Operating System 60 of the Serving Device 10 recalls the Computer File and/or Program 110 from Storage 100; places an electronic copy of the Computer File and/or Program 110 into RAM 80; and encrypts and transmits the Computer File and/or Program 110 to the Client Device 11 via the Communication Means 120. Then the Public Key Infrastructure 41 of the Operating System 61 of the Client Device 11 receives and decrypts from transmission, using encrypted communication protocols (such as, but not limited to, secure sockets layer (SSL), transport layer security (TLS), virtual private network (VPN), etc.), said Computer File and/or Program 110 and places an electronic copy of said Computer File and/or Program 110 into RAM 81. Then the Controlling Client Software and/or Firmware 31 automatically instructs the Encrypting File System 51 of the Client Device 11 to encrypt and save said electronic copy of the Computer File and/or Program 110 from RAM 81 to Storage 101, using the associated permissions and/or rights transmitted by the Serving Device 10, and to then erase any electronic copies of the Computer File and/or Program 110 from RAM 81. Then the Controlling Client Software and/or Firmware 31 of the Operating System 61 of the Client Device 11 instructs the Operating System 61 of the Client Device 11 to reestablish user intervention.

[0075] The user of the Client Device 11 may use the Computer File and/or Program 110 saved in Storage 101, subject to the permissions and/or rights associated therewith, as if said Computer File and/or Program 110 were not encrypted. Copies or moves of the Computer File and/or Program 110 which are not executed by the Encrypting File System 51, will not be properly encrypted for use on a computing device other than the Client Device 11. In accordance with said permissions and/or rights, the user of the Client Device 11 may utilize the Controlling Client Software and/or Firmware 31 to activate functionality of the Encrypting File System 51 to execute a move or copy of the Computer File and/or Program 110 from Storage 101 to Storage 102 of a Next Client Device 12. The Transceiver 72 of the Client Device 12 is connected to a Communication Means 120. The user of the Client Device 11 views a window (such as, but not limited to, as used by the windows 2000 operating system) of the Client Interface 21 and the Next Client Interface 22, which displays the relevant contents of Storage 101 to Storage 102, respectively, on the video display of the Client Device 11. The user iden-

tifies the object (such as, but not limited to, icon) (hereinafter "icon") associated with the Computer File and/or Program 110 to be moved from Storage 101 to Storage 102. The user of the Client Device 11 uses their computer mouse to move the icon (such as, but not limited to, a graphical user interface drag-n-drop move) associated with the Computer File and/or Program 110 from the Client Interface 21 window to the Next Client Interface 22 window. The drag-n-drop of said icon associated with said Computer File and/or Program 110 initiates a series of automated actions by the Controlling Serving Software and/or Firmware 30 then by the Controlling Client Software and/or Firmware 31. First, the Controlling Client Software and/or Firmware 31 instructs the Operating System 61 of the Client Device 11 to temporarily suspend user intervention to prevent any form of unauthorized data or instruction input into or throughout the Client Device 11 or the Next Client Device 12 by a means or mechanism internal or external to either the Client Device 11 or the Next Client Device 12, such as, but not limited to, user input or control through use of a keyboard, mouse or other physical means or mechanism; a computer program; macro; or any other means or mechanism which could in any way affect the functionality of the software and/or firmware of the present invention which could in any way affect the functionality of any software and/or firmware utilized by the present invention, and to prevent any form of unauthorized access to, use of, control over the Computer File and/or Program during execution of the transmission request. Then the Controlling Client Software and/or Firmware 31 instructs the Controlling Client Software and/or Firmware 32 to instruct the Operating System 62 of the Next Client Device 12 to temporarily suspend user intervention (such as, but not limited to, keyboard or mouse intervention, program or macro instructions, etc.) during execution of the transmission request. Then the Controlling Client Software and/or Firmware 32 instructs the Operating System 62 of the Next Client Device 12 to temporarily suspend user intervention. Then the Controlling Client Software and/or Firmware 32 instructs the Controlling Client Software and/or Firmware 31 to transmit said Computer File and/or Program 110 to the Next Client Device 12. Then the Controlling Client Software and/or Firmware 31 instructs the Encrypting File System 51 to recall and decrypt said Computer File and/or Program 110, and its associated permissions and/or rights, from Storage 101 and to save an electronic copy thereof in RAM 81. Then the Controlling Client Software and/or Firmware 31 instructs the Public Key Infrastructure 41 of the Operating System 61 of the Client Device 11 to encrypt and transmit the electronic copy of said Computer File and/or Program 110 from RAM 81, and its associated permissions and/or rights, to the Next Client Device 12 via Communication Means 120. Then the Controlling Client Software and/or Firmware 32 instructs the Public Key Infrastructure 42 of the Next Client Device 12 to receive and decrypt from transmission

File System 51 to encrypt the MP3 audio file.

[0078] Furthermore, the user of the Client Device 11 then decides to transfer the MP3 audio file to Next Client Device 12, and in this example, the user can do so based on the permissions and/or rights associated with the MP3 audio file. The user of the Client Device 11 connects the Transceiver 71 of the Client Device 11 to a Communication Means 120 with a subsequent communications connection to the Internet. The user of the Next Client Device 12 connects the Transceiver 72 of the Next Client Device 12 to a Communication Means 120 with a subsequent communications connection to the Internet. The user of the Client Device 11 views the Client Interface 21 and a copy of the Next Client Interface 22 on the video display of the Client Device 11, which displays the relevant contents of Storage 101 and Storage 102, respectively. The user identifies the object (such as, but not limited to, icon) (hereinafter "icon") associated with the MP3 audio file to be moved from Storage 101 to Storage 102. The user of the Client Device 11 uses its computer mouse to move the icon (such as, but not limited to, a graphical user interface drag-n-drop move) associated with the MP3 audio file from the Client Interface 21 window to the Next Client Interface 22 window. The drag-n-drop of said icon associated with the MP3 audio file initiates a series of automated actions by the Controlling Client Software and/or Firmware 31 then by the Controlling Client Software and/or Firmware 32. First, the Controlling Client Software and/or Firmware 31 instructs the Operating System 61 of the Client Device 11 to temporarily suspend user intervention (such as, but not limited to, keyboard or mouse intervention, program or macro instructions, etc.) during execution of the transmission request. Then the Controlling Client Software and/or Firmware 31 instructs the Controlling Client Software and/or Firmware 32 to instruct the Operating System 62 of the Next Client Device 12 to temporarily suspend user intervention (such as, but not limited to, keyboard or mouse intervention, program or macro instructions, etc.) during execution of the transmission request. Then the Controlling Client Software and/or Firmware 32 instructs the Operating System 62 of the Next Client Device 12 to temporarily suspend user intervention. Then the Controlling Client Software and/or Firmware 32 instructs the Controlling Client Software and/or Firmware 31 to transmit the MP3 audio file to the Next Client Device 12. Then the Controlling Client Software and/or Firmware 31 recalls the permissions and/or rights associated with the MP3 audio file and used by the Encrypting File System 51 and instructs the Encrypting File System 51 to recall and decrypt the MP3 audio file from Storage 101 and save an electronic copy thereof in Random Access Memory 81. Then the Controlling Client Software and/or Firmware 31 instructs the Public Key Infrastructure 41 of the Operating System 61 of the Client Device 11 to encrypt and transmit the electronic copy of the MP3 audio file from Random Access Memory 81, and its

associated permissions and/or rights, to the Next Client Device 12 via Communication Means 120. Then the Controlling Client Software and/or Firmware 32 instructs the Public Key Infrastructure 42 of the Next Client Device 12 to receive and decrypt from transmission the MP3 audio file, and its associated permissions and/or rights, and place an electronic copy thereof in Random Access Memory 82. In the case of a move of the MP3 audio file from Storage 101 to Storage 102, upon receipt of the MP3 audio file into Random Access Memory 82 by the Next Client Device 12, the Controlling Client Software and/or Firmware 32 of the Next Client Device 12 automatically instructs the Controlling Client Software and/or Firmware 31 of the Client Device 11 to instruct the Operating System 61 and/or the Encrypting File System 51 of the Client Device 11 to delete all copies of the MP3 audio file in Storage 101 or Random Access Memory 81. Then the Controlling Client Software and/or Firmware 31 instructs the Operating System 61 to reestablish user intervention of the Client Device 11. Then the Controlling Client Software and/or Firmware 32 automatically instructs the Encrypting File System 52 of the Operating System 62 of the Next Client Device 12 to encrypt and save to Storage 102 said electronic copy of the MP3 audio file from Random Access Memory 82, using the associated permissions and/or rights transmitted from the Client Device 11, and then erase all electronic copies of the MP3 audio file from Random Access Memory 82. Then the Controlling Client Software and/or Firmware 32 instructs the Operating System 62 to reestablish user intervention of the Next Client Device 12. At this point, the Controlling Client Software and/or Firmware 32 has concluded its portion of the transmission and encryption for storage process and the program related to the Controlling Client Software and/or Firmware 32 terminates. The user of the Next Client Device 12 is now able to play the MP3 audio file, however, in this example the user of the Client Device 11 is not able to play the MP3 audio file because the file was "moved" and during the "move" process, all copies of the MP3 audio file were erased from the Client Device 11 upon conclusion of the "move" process. Additionally, since the MP3 audio file has been encrypted by the Encrypting File System 51 for use on the Next Client Device 12, traditional moves or duplications of the MP3 audio file will not be authorized by the Encrypting File System 51 and only moves or duplications of the MP3 audio file utilizing the Controlling Client Software and/or Firmware 32 will be authorized by the Encrypting File System 51.

[0079] "Means or mechanism" herein refers to 35 U.S.C. Section 112, paragraph 6. The term "means" of "means or mechanism" is subject to 35 U.S.C. Section 112, paragraph 6, while the term "mechanism" of "means or mechanism" is not subject to 35 U.S.C. Section 112, paragraph 6.

[0080] Although the invention has been described in detail in the foregoing embodiments for the purpose

and the encrypted permissions and/or rights and temporarily suspends user intervention of the next client device while the encrypted computer file and/or program is received by the next client device.

15. A system as described in Claim 14 wherein the connector includes a communication link, the server device includes a transmitter connected to the communication link for transferring the encrypted computer file and/or program and unencrypted permissions and/or rights to the communication link, and the client device includes a receiver connected to the communication link which receives the encrypted computer file and/or program and the encrypted permissions and/or rights from the communication link.

16. A system as described in Claim 15 wherein the first and second connectors are part of the Internet or other communication network.

17. A method for manipulating a computer file and/or program comprising the steps of:

suspending intervention by a user at a client device of the client device;

encrypting an unencrypted computer file and/or program at the server device to form an encrypted computer file and/or program;

transferring the encrypted computer file and/or program to the client device along a connector connected to the client device and the server device; and

reestablishing the intervention of the client device by the user.

18. A method as described in Claim 17 including before the transferring step, there is the step of encrypting permissions and/or rights of the unencrypted computer file and/or program and transferring the encrypted permission and/or rights to the client device along the connector from the server device.

19. A method as described in Claim 18 including before the encrypting the unencrypted computer file and/or program step, there is the step of requesting by the client device the unencrypted computer file and/or program of the server device.

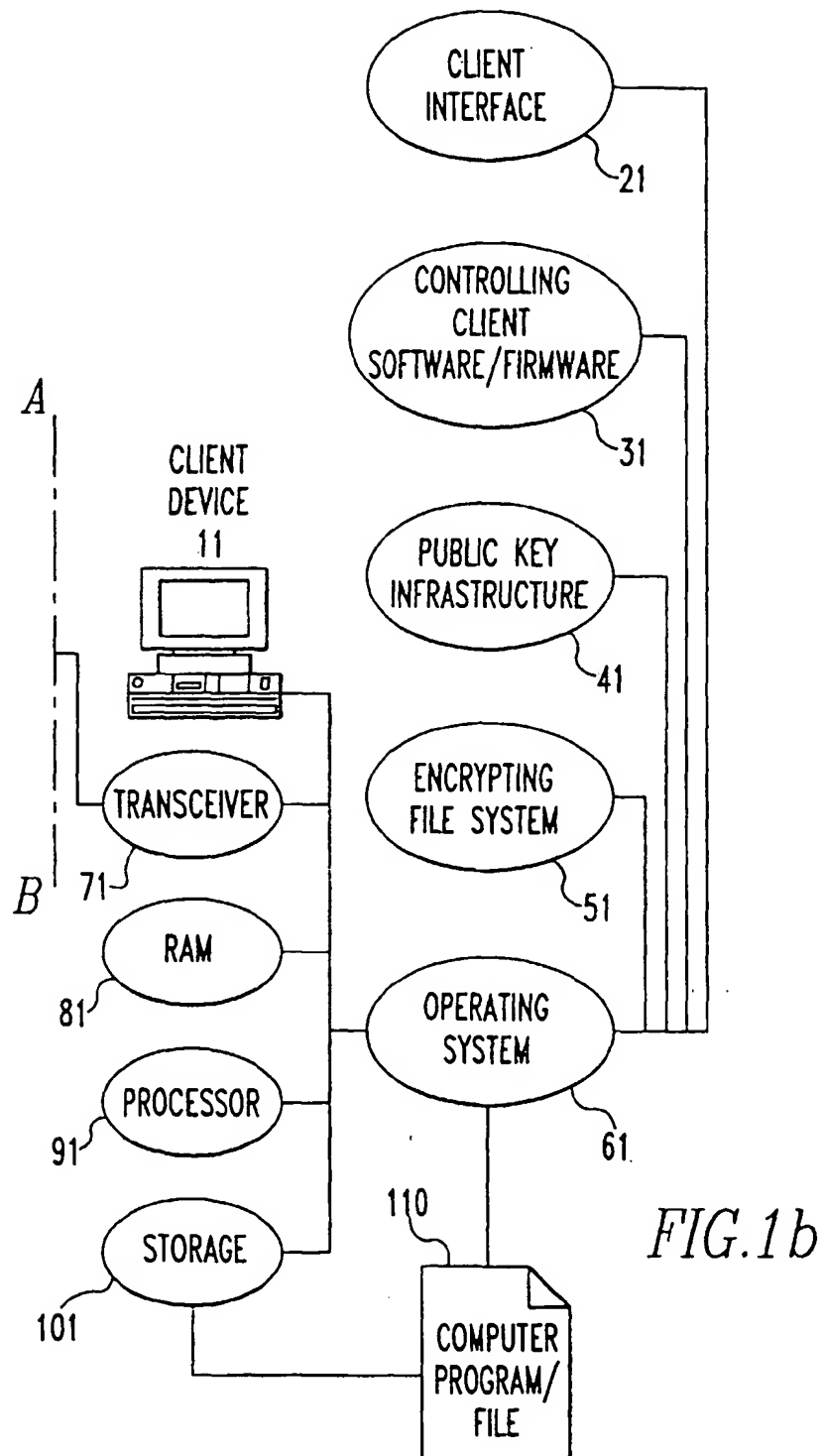
20. A method as described in Claim 19 including after the requesting step, there is the step of copying a primary unencrypted computer file and/or program to form the unencrypted computer file and/or program.

21. A method as described in Claim 20 including before the reestablishing step, there is the step of decrypt-

ing the encrypted computer file and/or program back to the unencrypted computer file and/or program at the client device.

22. A method as described in Claim 21 including after the decrypting step, there are the steps of encrypting the unencrypted computer file and/or program and permissions and/or rights at the client device and storing the encrypted computer program and/or file and the encrypted permissions and/or rights in the client device.

23. A method as described in Claim 22 including after the storing step, there is the step of transferring the encrypted computer file and/or program to a next client device connected to the client device by a second connector.



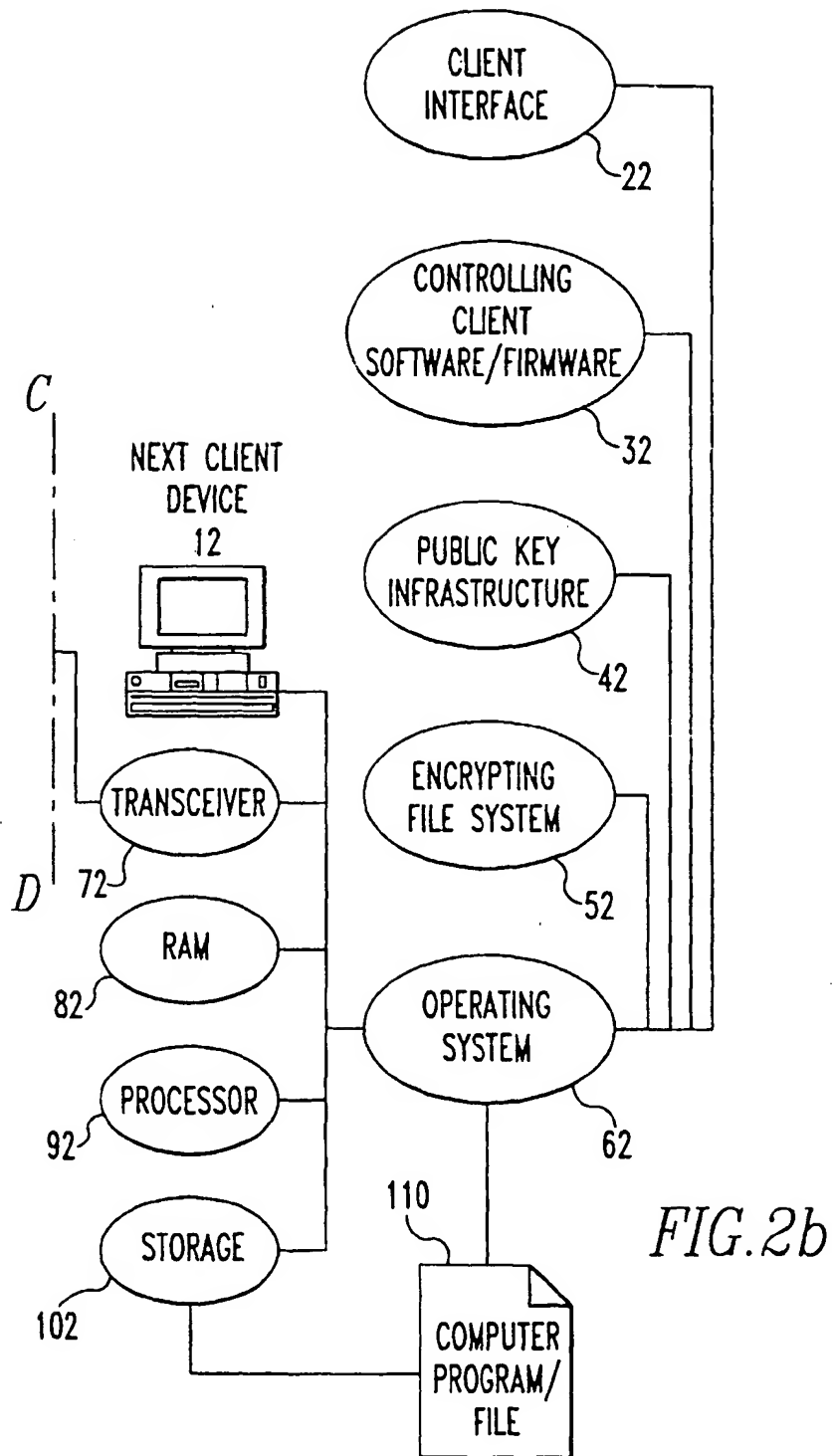


FIG.2b

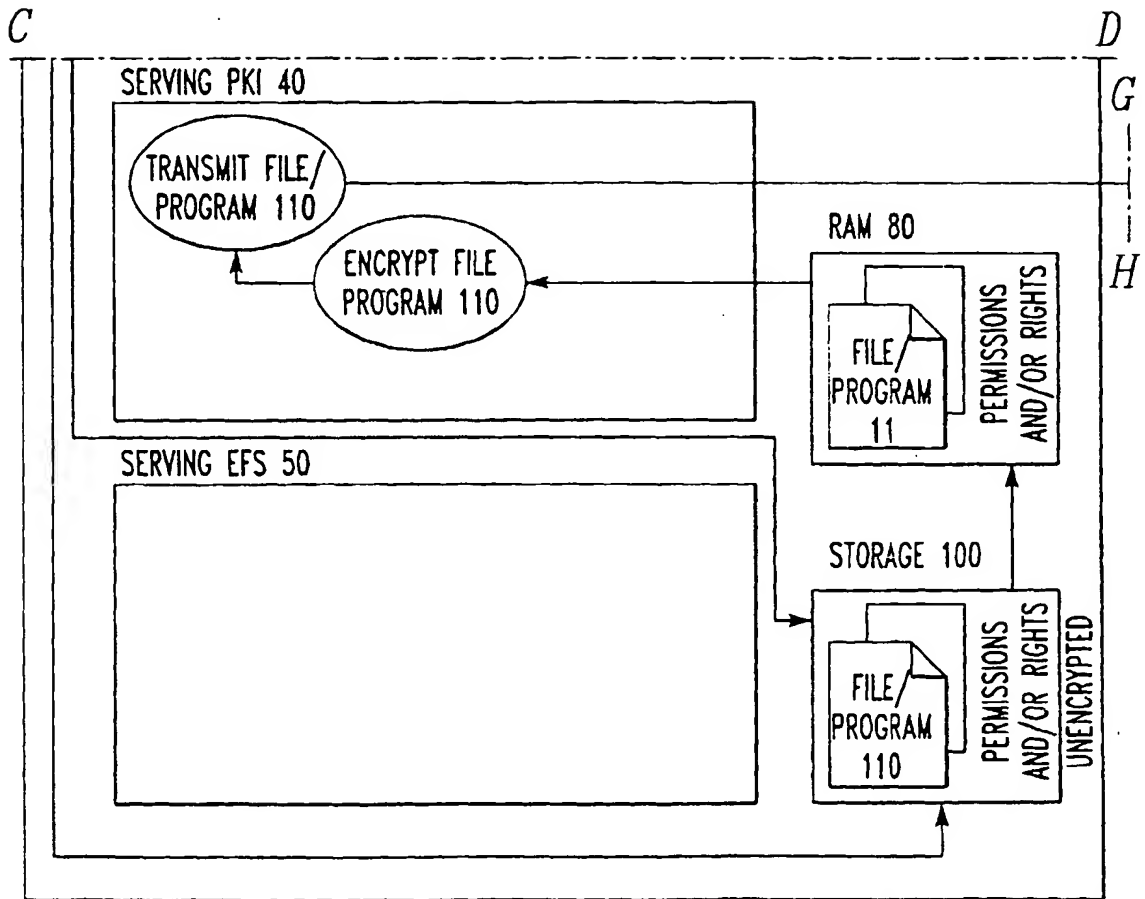


FIG. 3b

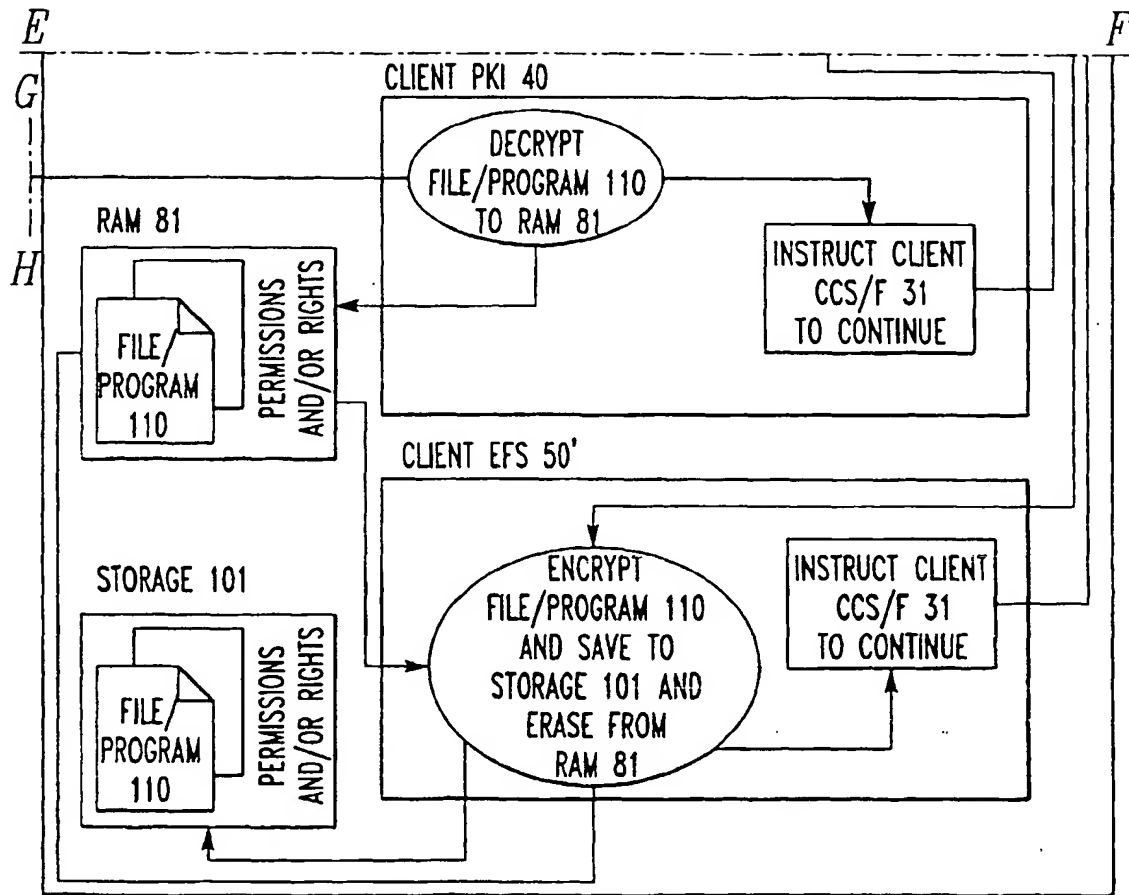


FIG. 3d

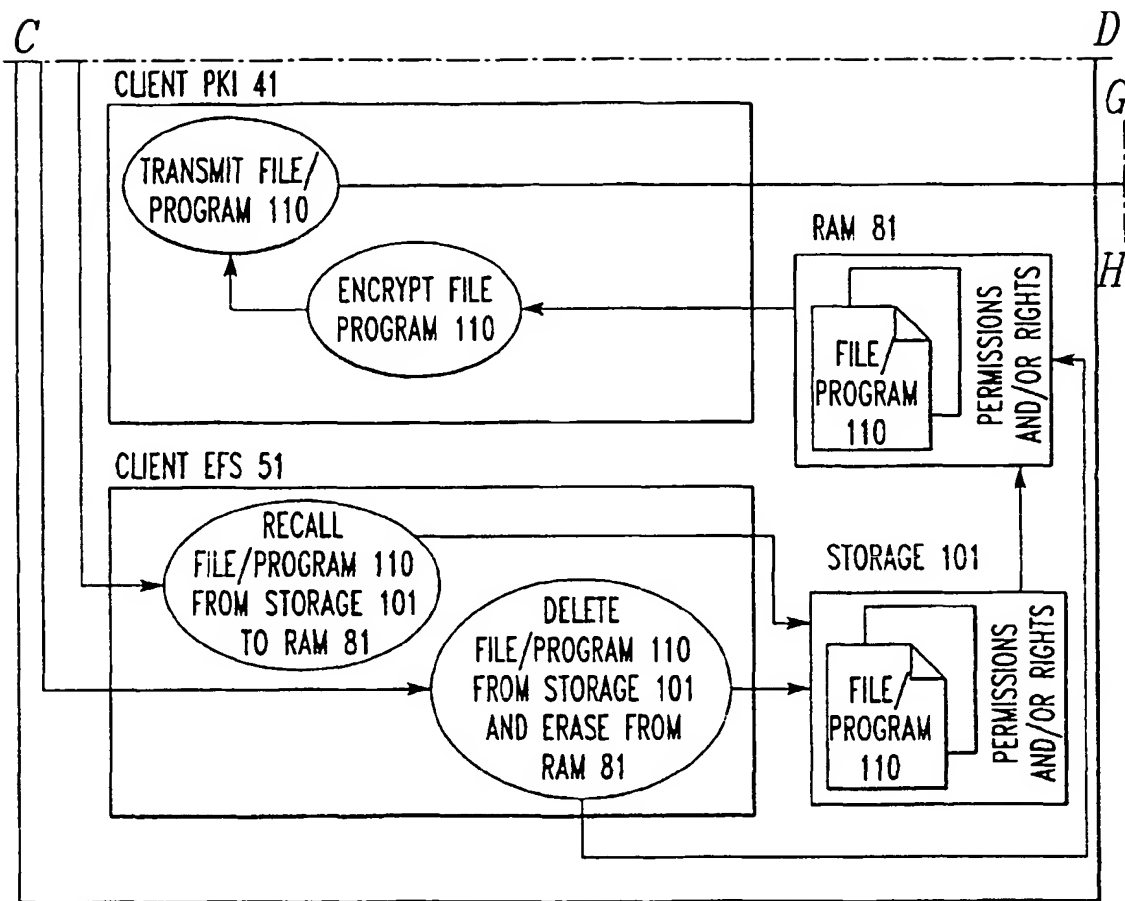


FIG. 4b

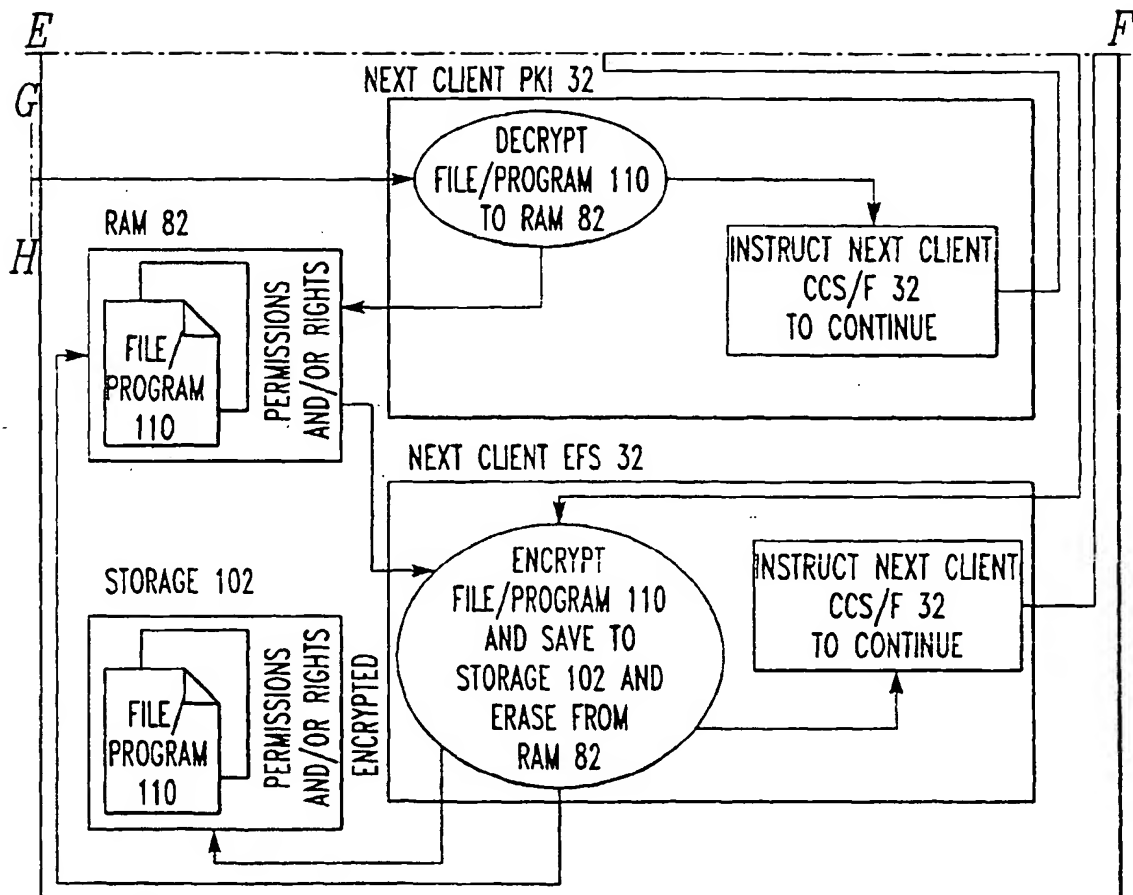


FIG. 4d

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 031 909 A3

(12)

EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
02.04.2003 Bulletin 2003/14

(51) Int Cl.7: G06F 1/00

(43) Date of publication A2:
30.08.2000 Bulletin 2000/35

(21) Application number: 00300727.5

(22) Date of filing: 31.01.2000

(84) Designated Contracting States:
AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: Hair, Arthur R.
Upper St. Clair, PA 15241 (US)

(74) Representative: O'Connell, David Christopher
Haseltine Lake & Co.,
Imperial House,
15-19 Kingsway
London WC2B 6UD (GB)

(30) Priority: 23.02.1999 US 256432

(71) Applicant: Sightsound.Com Incorporated
Mt. Lebanon, PA 15228 (US)

(54) A system and method for manipulating a computer file and/or program

(57) A system for manipulating a computer file and/or program. The system includes a serving device having access to a computer file and/or program which is unencrypted and which can encrypt the unencrypted computer file and/or program to become an encrypted computer file and/or program and transfer it. The system includes a connector connected to the serving device on which the encrypted computer file and/or program travels and to which the serving device transfers the encrypted computer file and/or program. The system includes a client device which receives the encrypted computer file and/or program and decrypts the encrypted computer file and/or program back to the unencrypted computer file and/or program. The client device does not allow intervention to the encrypted computer file and/or program during a time when the encrypted computer and/or file program is received. The serving device is separate, apart and distinct from the client device. A method for manipulating a computer file and/or program. The method includes the steps of suspending intervention by a user at a client device of the client device. Then there is the step of encrypting an unencrypted computer file and/or program at the server device to form an encrypted computer file and/or program. Next there is the step of transferring the encrypted computer file and/or program to the client device along a connector connected to the client device and the server device. Then there is the step of reestablishing the intervention of the client device by the user.

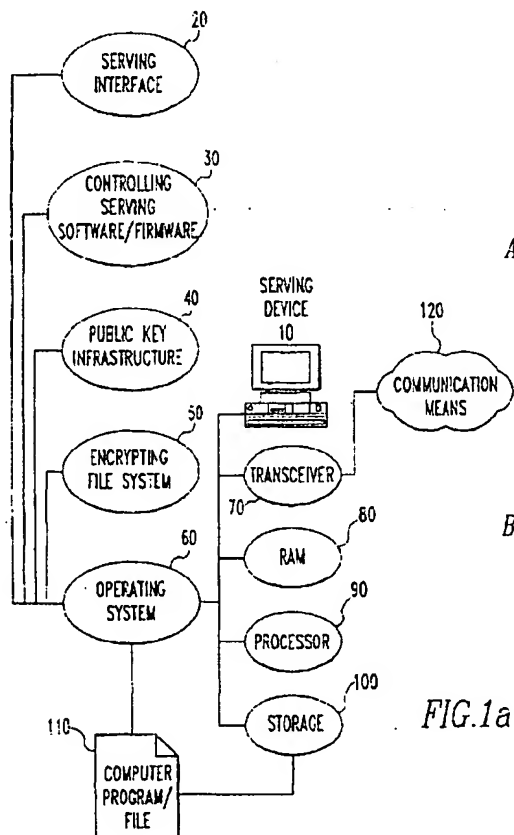


FIG.1a

EP 1 031 909 A3



European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 00 30 0727

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim:	CLASSIFICATION OF THE APPLICATION (Int.C1.7)
X	US 5 666 411 A (MCCARTY JOHNNIE C) 9 September 1997 (1997-09-09) * abstract * * column 5, line 1 - column 6, line 21 * * column 6, line 52 - line 64 * * column 11, line 5 - line 25 * * figures 1-4 *	1, 17	G06F1/00
Y	---	2-16, 18-23	
Y	US 5 845 281 A (BENSON GREG ET AL) 1 December 1998 (1998-12-01) * abstract *	2-16, 18-23	
A	EP 0 881 561 A (HEWLETT PACKARD CO) 2 December 1998 (1998-12-02) * the whole document *	1-23	
			TECHNICAL FIELDS SEARCHED (Int.C1.7)
			G06F
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		5 February 2003	Sigolo, A
<p>CATEGORY OF CITED DOCUMENTS</p> <p>X: particularly relevant if taken alone Y: particularly relevant if combined with another document of the same category A: technological background O: non-written disclosure P: intermediate document</p> <p>T: theory or principle underlying the invention E: earlier patent document, but published on or after the filing date D: document cited in the application L: document cited for other reasons 8: member of the same patent family, corresponding document</p>			